

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-148593

(P2000-148593A)

(43) 公開日 平成12年5月30日 (2000.5.30)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
G 0 6 F 12/14	3 1 0	G 0 6 F 12/14	3 1 0 Z
12/16	3 2 0	12/16	3 2 0 B
15/00	3 3 0	15/00	3 3 0 A
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 D
	6 6 0		6 6 0 E

審査請求 未請求 請求項の数12 O L (全 20 頁) 最終頁に続く

(21) 出願番号 特願平11-242712
(22) 出願日 平成11年8月30日 (1999.8.30)
(31) 優先権主張番号 特願平10-244719
(32) 優先日 平成10年8月31日 (1998.8.31)
(33) 優先権主張国 日本 (J P)

(71) 出願人 000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目6番地
(72) 発明者 洲崎 誠一
神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内
(72) 発明者 豊島 久
東京都江東区新砂一丁目6番27号 株式会社日立製作所公共情報事業部内
(74) 代理人 100075096
弁理士 作田 康夫

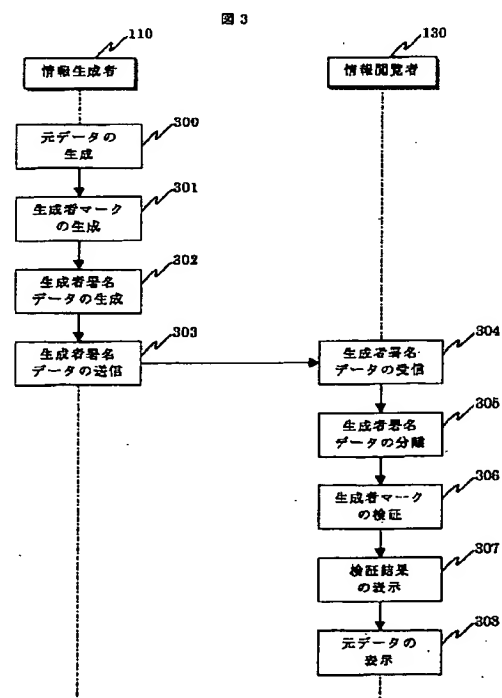
最終頁に続く

(54) 【発明の名称】 情報の認証システム

(57) 【要約】

【課題】 第一のユーザが生成したマルチメディアデータの真正性を、第二のユーザが視覚、聴覚などによって確認可能とする。

【解決手段】 情報生成者110は、アプリケーションプログラムを使って情報閲覧者130に伝達する元データを生成する。次に、該元データの真正性を保証する生成者マークを生成し、当該元データと生成者マークとを一つに纏めて生成者署名データを生成する。そして、該生成者署名データを情報閲覧者130に送信する。生成者署名データを受け取った情報閲覧者130は、該生成者署名データを元データと生成者マークとに分離し、該生成者マークが確かに情報生成者110によって生成されたものであるか否かを検証する。そして、該検証結果を視覚、聴覚などによって確認するとともに、元データを適切なアプリケーションプログラムによって確認する。



段が、前記第二のマルチメディアデータの生成時に含めた、前記第一のマルチメディアデータの真正性を保証する証拠データを用いて行われるものであることを特徴とする情報の認証システム。

【請求項 6】請求項 1 に記載された情報の認証システムであって、前記第一のマルチメディアデータの真正性を保証する前記第二のマルチメディアデータは、前記第一のマルチメディアデータまたはその圧縮子に対して施されたデジタル署名を含むことを特徴とする情報の認証システム。

【請求項 7】請求項 6 記載の情報の認証システムであって、前記第一のマルチメディアデータの真正性を保証する前記第二のマルチメディアデータは、前記第一のマルチメディアデータまたはその圧縮子に対して施されたデジタル署名に加えて、該デジタル署名を検証する際に使用する公開鍵、または電子認証書を含むことを特徴とする情報の認証システム。

【請求項 8】請求項 1 に記載された情報の認証システムであって、前記第二のマルチメディアデータを用いて前記第一のマルチメディアデータの真正性を検証する手段は、視覚または聴覚によって確認できることを特徴とする情報の認証システム。

【請求項 9】請求項 1 に記載された情報の認証システムであって、前記第二のマルチメディアデータを用いて前記第一のマルチメディアデータの真正性が確認された場合に、該第一のマルチメディアデータを閲覧可能にすることを特徴とする情報の認証システム。

【請求項 10】請求項 3 記載の情報の認証システムであって、前記情報生成用端末が、前記情報認証用端末に送付するデータは、前記第一のマルチメディアデータの圧縮子であることを特徴とする情報の認証システム。

【請求項 11】請求項 6 に記載された情報の認証システムであって、前記第二のマルチメディアデータを生成する場合に、前記第一のマルチメディアデータに関連する属性情報をもデジタル署名の対象とすることを特徴とする情報の認証システム。

【請求項 12】請求項 11 記載の情報の認証システムであって、前記属性情報に、前記第一のマルチメディアデータに対するアクセス制御情報が含まれており、前記第一のマルチメディアデータの閲覧の可否を、該アクセス制御情報を用いて決定することを特徴とする情報の認証システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、第一のユーザが生成した様々な種類のマルチメディアデータを、第二のユーザが入手・閲覧する情報システムにおいて、第二のユーザが当該マルチメディアデータの真正性を確認することができる認証システムに関する。

【0002】

【従来の技術】パーソナルコンピュータのような情報機器の普及と通信ネットワークの整備に伴い、様々な情報が電子化され、ネットワークを介してやり取りされるようになってきている。このようなネットワークを介した情報のやり取りは、遠く離れた人とでも簡単、かつ高速に行うことができる反面、①通信データを第三者に盗聴される、②通信データを第三者に改ざんされる、③通信相手が自称する本人でない、などといった危険がある。

【0003】これらの危険から情報システムを守るために、従来より暗号、認証などといったセキュリティ技術が広く用いられている。具体的には、前記第一の課題に対しては通信データを暗号化する。また、前記第二、第三の課題に対しては通信データにデジタル署名を付加する。

【0004】このようなデジタル署名技術の概要については、例えば「Cryptography and Data Security (著者: Dorothy Elizabeth Robling Dennin g, 発行所: ADDISON-WESLEY PUBLISHING COMPANY)」の 14 ページから 16 ページに記載されている。

【0005】デジタル署名は、公開鍵暗号方式における暗号鍵の非対称性を利用した技術である。あるデータに対してデジタル署名を付加する方法、および、該デジタル署名付きデータを検証する方法は、以下の通りである。

【0006】データを生成した第一のユーザは、まず、生成したデータを自分の秘密鍵（第一のユーザが正しい値を知っている暗号鍵）で暗号化して暗号文（デジタル署名）を生成する。次に元データとデジタル署名とを組にし、第二のユーザに渡す。第二のユーザは、デジタル署名を上記第一のユーザの公開鍵（上記秘密鍵と一対一対応の関係にあり、第二のユーザも含めて、全てのユーザに対して正しい値が公開されている暗号鍵）で復号し、その結果と元データとを比較する。そして、復号結果と元データとが一致していた場合に、当該データを生成したのが第一のユーザ本人に間違いなく、かつ、当該データが改ざんされていないものと判断する。

【0007】なぜなら、もし、不正を行おうとしている第三のユーザが生成したデータ、あるいは、該第三のユーザによって改ざんが加えられたデータであれば、デジタル署名を第一のユーザの公開鍵で復号した結果と元データとが一致しないからである。言い換えれば、デジタル署名を第一のユーザの公開鍵で復号した結果と元データが一致するということは、当該デジタル署名を生成する際に、当該公開鍵を対応した第一のユーザの秘密鍵を用いたはずであり、第一のユーザの秘密鍵を用いることができるのは第一のユーザ本人だからである。

【0008】上述のとおり、デジタル署名技術を用いることにより、データの生成者は、当該データを生成し

たのが本人に間違いないこと、および当該データが改ざんされていないこと（本発明では、両性質をまとめて当該データの真正性と呼ぶ）を第三者に対して証明することができる。しかし、デジタル署名自体は単なる数値データであり、その内容を人が見て直接解釈することは困難である。

【0009】一方、多くの人は何かを見た場合に、そのものが示す意味までも暗黙のうちに意識する。例えば、ブラウザプログラムを使って、インターネット上で公開された販売店のWebページを閲覧した場合に、もし、当該Webページに、あるクレジットカード会社のロゴマークが貼り付けられていたら、多くの閲覧者は当該販売店が当該クレジットカード会社の加盟店であり、その会社のクレジットカードで支払い処理を行うことができると判断することは容易に予想される。また、ワードプロセッサなどで生成された電子文書に、サインや印影などの画像データが貼付されていたら、当該サインや印影の対象者が当該データを生成した、あるいは当該データの内容を承認したと判断するものと考えられる。

【0010】しかし、上記ロゴマークやサイン、印影などは単なる画像データであり、何ら証拠性（当該データが、貼付された画像データが意味する内容と合致していることに対する保証）を持つものではない。なぜなら、第一の情報（Webページや電子文書など）に貼付された画像データをコピーし、第二の情報に貼付することは、第一のデータの生成者だけでなく全ての人にとって容易だからである。

【0011】そこで、デジタル署名が正しく検証された場合に、サインや印影などの画像データを表示するように制御することで証拠性を保つ、デジタル署名システムが考案されている。このようなデジタル署名システムについては、例えば米国特許5,606,609「ELECTRONIC DOCUMENT VERIFICATION SYSTEM AND METHOD」に記載されている。

【0012】

【発明が解決しようとする課題】ところで、現在の情報システムでは、様々な処理を電子的に行うために、テキストデータやワードプロセッサ文書、Webページ、図面、音声データ、画像データ、あるいはビデオデータなどといった多種多様なマルチメディアデータを取り扱うことが必要となっている。しかし、それらのマルチメディアデータは、それぞれ異なるデータ形式（データフォーマット）を有している。例えば、テキストデータはテキスト形式と呼ばれるデータフォーマットであり、Webページの多くはHTML形式と呼ばれるデータフォーマットである。さらに、画像データには、ビットマップ形式やJPEG形式、GIF形式などと呼ばれるいくつかのデータフォーマットを使うことが可能であり、ワードプロセッサ文書などは、それを処理するアプリケーション

プログラム（ワードプロセッサ）独自のデータフォーマットを有している。

【0013】現在の情報システムでは、上記データフォーマットの異なるマルチメディアデータを適切に処理するために様々なアプリケーションプログラムが併用されている。例えば、あるアプリケーションプログラムではテキストフォーマットのデータを処理し、別のアプリケーションプログラムでは、当該アプリケーションプログラム独自のデータフォーマットのデータを処理している。また、さらに別のアプリケーションプログラムでは、複数種類のデータフォーマットのデータを処理することも可能である。

【0014】このように、多種多様なデータフォーマットを有するマルチメディアデータを、多くのアプリケーションプログラムを使い分けることによって処理するような環境において、前記従来のデジタル署名技術を用いてデータの真正性を保証する場合、以下のような問題がある。

【0015】上記環境において全てのマルチメディアデータの真正性を確認できるようにするためには、使用する全てのアプリケーションプログラムがデジタル署名を生成・検証するための機能を持たなければならない。しかし、現在、多くのアプリケーションプログラムはデジタル署名機能を有していない。そのため、たとえば、あるアプリケーションプログラムを用いて生成したマルチメディアデータにデジタル署名を付加した場合、新たに生成された署名付きマルチメディアデータのフォーマットは、元のマルチメディアデータのフォーマットとは異なるので、上記作成時に用いたアプリケーションプログラムでは処理できなくなってしまう。

【0016】さらに、既存のアプリケーションプログラムにデジタル署名機能を追加するには、全てのアプリケーションプログラム開発者（開発企業）の協力が必要であり、実際にはきわめて困難である。

【0017】また、前述のように、人は目で見えたもの、あるいは音として聞いたものが示す意味を暗黙のうちに意識する傾向にある。したがって、単なるデジタル署名技術を適用するだけでなく、デジタル署名の検証結果を視覚、聴覚などで直接的に確認できるようにしたほうが便利である。

【0018】本発明は、上記事情に鑑みてなされたものであり、本発明の目的は、テキストデータやワードプロセッサ文書、Webページ、図面、音声データ、画像データ、あるいはビデオデータなどといったいくつかの異なるデータフォーマットを有するマルチメディアデータを取り扱う情報システムにおいて、当該データフォーマットやそれらマルチメディアデータを処理するアプリケーションプログラムに依存することなく、第一のユーザが生成したマルチメディアデータの真正性を、第二のユーザが視覚、聴覚などで直接的に確認することができる認

証方法、およびそれを用いたシステム、さらには、該システムで使われる個々の装置と、それらを動作させるプログラムと、該システムに適したデータ構造を提供することである。

【0019】

【課題を解決するための手段】上記課題を解決するために、本発明では、第一のユーザが生成した第一のマルチメディアデータと、視覚、聴覚で確認できる性質と真正性検証手段とを備えた第二のマルチメディアデータを組にして、第三のマルチメディアデータを生成し、第二のユーザは、第三のマルチメディアデータを第一のマルチメディアデータと第二のマルチメディアデータとに分離した後、第二のマルチメディアデータが備える、視覚、聴覚で確認できる性質と真正性検証手段とを用いて、第一のマルチメディアデータが真正なものであるか否かを、視覚、聴覚によって確認するとともに、第一のマルチメディアデータを適切なアプリケーションプログラムを用いて処理することの特徴とする。

【0020】本発明によれば、まず、第一のユーザが任意のアプリケーションプログラムを用いて生成した第一のマルチメディアデータが真正なものであるか否かという証拠、すなわち、第二のマルチメディアデータを、第一のユーザ、あるいは全てのユーザが信頼する第三者（第三者機関）が生成したのち、該第一、第二のマルチメディアデータを組にして第三のマルチメディアデータを生成するようにしている。さらに、第二のユーザは、第三のマルチメディアデータを第一のマルチメディアデータと第二のマルチメディアデータとに分離した後、第二のマルチメディアデータが有する、視覚、聴覚で確認できる性質と真正性検証手段とを用いて第一のマルチメディアデータの真正性を視覚、聴覚で確認するようにしている。加えて、第一のマルチメディアデータを適切なアプリケーションプログラム、すなわち、第二のユーザが使用可能なアプリケーションプログラムの中で、第一のマルチメディアデータのデータフォーマットを処理可能なアプリケーションプログラムを用いて、該第一のマルチメディアデータを処理するようにしている。

【0021】すなわち、本発明の情報の認証システムは、情報生成用端末と、情報閲覧用端末と、が通信網を介して相互に接続されており、情報生成用端末は、情報閲覧用端末に伝達する第一のマルチメディアデータを生成する手段と、第一のマルチメディアデータの真正性を保証する第二のマルチメディアデータを生成する手段と、第一のマルチメディアデータと第二のマルチメディアデータとから第三のマルチメディアデータを生成し、該第三のマルチメディアデータを情報閲覧用端末に送付する手段とを備え、情報閲覧用端末は、情報生成用端末から送付された第三のマルチメディアデータを受け取り、該第三のマルチメディアデータから、第一のマルチメディアデータと、第二のマルチメディアデータとを分

離する手段と、第二のマルチメディアデータを用いて、第一のマルチメディアデータの真正性を検証する手段と、第一のマルチメディアデータを閲覧可能とする手段とを備えることを特徴としている。

【0022】また、本発明の情報の認証システムは、情報生成用端末と、情報閲覧用端末と、ゲートウェイ装置と、が通信網を介して相互に接続されており、情報生成用端末は、情報閲覧用端末に伝達する第一のマルチメディアデータを生成する手段と、第一のマルチメディアデータの真正性を保証する第二のマルチメディアデータを生成する手段と、第一のマルチメディアデータと第二のマルチメディアデータとから第三のマルチメディアデータを生成し、該第三のマルチメディアデータを、ゲートウェイ装置を介して情報閲覧用端末に送付する手段とを備え、ゲートウェイ装置は、情報生成用端末から送付された第三のマルチメディアデータを受け取り、該第三のマルチメディアデータから、第一のマルチメディアデータと、第二のマルチメディアデータとを分離する手段と、第二のマルチメディアデータを用いて、第一のマルチメディアデータの真正性を検証する手段と、第一のマルチメディアデータと、第二のマルチメディアデータと、真正性の検証処理の結果とを情報閲覧用端末に送付する手段とを備え、情報閲覧用端末は、ゲートウェイ装置から送付された第一のマルチメディアデータと、第二のマルチメディアデータと、真正性の検証処理の結果とを受け取り、該三種のデータを閲覧可能とする手段とを備えることを特徴としている。

【0023】また、本発明の情報の認証システムは、情報生成用端末と、情報認証用端末と、情報閲覧用端末と、が通信網を介して相互に接続されており、情報生成用端末は、第一のマルチメディアデータを生成する手段と、第一のマルチメディアデータを情報認証用端末に送付する手段と、情報認証用端末から返送された第三のマルチメディアデータを受け取り、該第三のマルチメディアデータを情報閲覧用端末に送付する手段とを備え、情報認証用端末は、情報生成用端末から送付された第一のマルチメディアデータを受け取り、該第一のマルチメディアデータの真正性を保証する第二のマルチメディアデータを生成する手段と、第一のマルチメディアデータと第二のマルチメディアデータとから第三のマルチメディアデータを生成し、該第三のマルチメディアデータを情報生成用端末に返送する手段とを備え、閲覧用端末の端末は、情報生成用端末から送付された第三のマルチメディアデータを受け取り、該第三のマルチメディアデータから、第一のマルチメディアデータと、第二のマルチメディアデータとを分離する手段と、第二のマルチメディアデータを用いて、第一のマルチメディアデータの真正性を検証する手段と、第一のマルチメディアデータを閲覧する手段とを備えていることを特徴としている。

【0024】また、本発明の情報の認証システムは、情

報生成用端末と、情報認証用端末と、情報閲覧用端末と、ゲートウェイ装置と、が通信網を介して相互に接続されており、情報生成用端末は、第一のマルチメディアデータを生成する手段と、第一のマルチメディアデータを情報認証用端末に送付する手段と、情報認証用端末から返送された第三のマルチメディアデータを受け取り、該第三のマルチメディアデータをゲートウェイ装置を介して情報閲覧用端末に送付する手段とを備え、情報認証用端末は、情報生成用端末から送付された第一のマルチメディアデータを受け取り、該第一のマルチメディアデータの真正性を保証する第二のマルチメディアデータを生成する手段と、第一のマルチメディアデータと第二のマルチメディアデータとから第三のマルチメディアデータを生成し、該第三のマルチメディアデータを情報生成用端末に返送する手段とを備え、ゲートウェイ装置は、情報生成用端末から送付された第三のマルチメディアデータを受け取り、該第三のマルチメディアデータから、第一のマルチメディアデータと、第二のマルチメディアデータとを分離する手段と、第二のマルチメディアデータを用いて、第一のマルチメディアデータの真正性を検証する手段と、第一のマルチメディアデータと、第二のマルチメディアデータと、真正性の検証処理の結果とを情報閲覧用端末に送付する手段とを備え、情報閲覧用端末は、ゲートウェイ装置から送付された第一のマルチメディアデータと、第二のマルチメディアデータと、真正性の検証処理の結果とを受け取り、該三種のデータを閲覧可能とする手段とを備えることを特徴としている。

【0025】さらに、本発明の情報の認証システムは、第二のマルチメディアデータを用いて、第一のマルチメディアデータの真正性を検証する手段が、第二のマルチメディアデータの生成時に含めた、第一のマルチメディアデータの真正性を保証する証拠データを用いて行われるものであることを特徴としている。

【0026】さらに、本発明の情報の認証システムは、第一のマルチメディアデータの真正性を保証する第二のマルチメディアデータは、第一のマルチメディアデータまたはその圧縮子に対して施されたデジタル署名を含むことを特徴としている。

【0027】さらに、本発明の情報の認証システムは、第一のマルチメディアデータの真正性を保証する第二のマルチメディアデータは、第一のマルチメディアデータまたはその圧縮子に対して施されたデジタル署名に加えて、該デジタル署名を検証する際に使用する公開鍵、または電子認証書を含むことを特徴としている。

【0028】さらに、本発明の情報の認証システムは、第二のマルチメディアデータを用いて第一のマルチメディアデータの真正性を検証する手段は、視覚または聴覚によって確認できることを特徴としている。

【0029】さらに、本発明の情報の認証システムは、第二のマルチメディアデータを用いて第一のマルチメデ

ィアデータの真正性が確認された場合に、該第一のマルチメディアデータを閲覧可能にすることを特徴としている。

【0030】さらに、本発明の情報の認証システムは、情報生成用端末が、情報認証用端末に送付するデータは、第一のマルチメディアデータの圧縮子であることを特徴としている。

【0031】さらに、本発明の情報の認証システムは、第二のマルチメディアデータを生成する場合に、第一のマルチメディアデータに関連する属性情報をもデジタル署名の対象とすることを特徴としている。

【0032】さらに、本発明の情報の認証システムは、属性情報に、第一のマルチメディアデータに対するアクセス制御情報が含まれており、第一のマルチメディアデータの閲覧の可否を、該アクセス制御情報を用いて決定することを特徴としている。

【0033】また、本発明による真正性保証プログラムは、真正性保証データの生成指示を受けた場合に、第一のマルチメディアデータの真正性を保証する第二のマルチメディアデータを生成した後、該第一のマルチメディアデータと該第二のマルチメディアデータとから第三のマルチメディアデータを生成する手段、または、真正性保証データの検証指示を受けた場合に、受け取った第三のマルチメディアデータを、第一のマルチメディアデータと第二のマルチメディアデータとに分離した後、該第二のマルチメディアデータの真正性検証手段を用いて、該第一のマルチメディアデータの真正性を検証するとともに、視覚または、聴覚によって確認可能な方法により該検証結果を出力する手段を備えることを特徴としている。

【0034】また、本発明による真正性保証プログラムは、第三のマルチメディアデータの生成は、第一のマルチメディアデータと第二のマルチメディアデータに関する情報に基づいてヘッダ情報を生成した後、該ヘッダ情報と第一と第二のマルチメディアデータとを結合することによって行い、第三のマルチメディアデータの分離は、ヘッダ情報に基づいて第一のマルチメディアデータと第二のマルチメディアデータとを抽出することによって行うことを特徴としている。

【0035】さらに、本発明による真正性保証プログラムは、第三のマルチメディアデータの生成は、第一のマルチメディアデータに第二のマルチメディアデータに対するリンク情報を示すタグを追加することによって行ない、第三のマルチメディアデータの分離は、リンク情報を抽出することによって行うことを特徴としている。

【0036】さらに、本発明による真正性保証プログラムは、該真正性保証プログラムが動作する端末において、第一のマルチメディアデータを処理可能なアプリケーションプログラムが存在した場合には、該アプリケーションプログラムに第一のマルチメディアデータを渡し

て、該アプリケーションプログラムを起動することを特徴としている。

【0037】さらに、本発明による真正性保証プログラムは、真正性保証データの検証を開始する際の指示が第三のマルチメディアデータを受け取ることであることを特徴としている。

【0038】さらに、本発明による真正性保証プログラムは、真正性保証データの検証を開始する際の指示が閲覧用端末の利用者からによる明示的な命令であることを特徴としている。

【0039】また、本発明によるマルチメディアデータは、情報生成用端末が生成した第一のマルチメディアデータと、第一のマルチメディアデータの真正性を保証する第二のマルチメディアデータと、第一のマルチメディアデータと第二のマルチメディアデータとを分離するために必要な属性情報と、からなることを特徴としている。

【0040】さらに、本発明によるマルチメディアデータは、第二のマルチメディアデータに対するリンク情報を示すタグが、該第二のマルチメディアデータに証拠データが含まれることを明示的に示すものであることを特徴としている。

【0041】したがって、本発明によれば、第一のマルチメディアデータのデータフォーマットや、第一のマルチメディアデータを生成する際に第一のユーザが使用したアプリケーションプログラムに依存することなく、第二のユーザが、第二のマルチメディアデータの真正性検証手段を用いて、第一のマルチメディアデータの真正性を視覚、聴覚などで正しく確認することができる。

【0042】

【発明の実施の形態】以下、図面を用いて、本発明の実施例を説明する。なお、以下で説明する図面において、同一の番号は同様の部品・要素を表すものとする。また、これにより本発明が限定されるものではない。

【0043】図1は、本発明の第一の実施形態が適用された認証システムの概略構成を示す図である。本実施形態の認証システムは、各種マルチメディアデータ（前述の第一のマルチメディアデータ、以下、単に元データと称する）を生成する情報生成者110と、元データの真正性を保証するマルチメディアデータ（情報認証者110が生成する前述の第二のマルチメディアデータ、以下、単に認証者マークと称する）を発行する情報認証者120と、情報生成者110が生成した元データを閲覧する情報閲覧者130とが利用するシステムであって、図1に示すように、端末140₁～140₃（以下、単に端末140とも称する）が通信網100を介して、互いに接続された構成になっている。

【0044】端末140₁は、情報生成者110が使用する端末である。情報生成者110は、端末140₁を使って、元データを生成したり、元データの真正性を保

証するマルチメディアデータ（情報生成者110が生成する前述の第二のマルチメディアデータ、以下、単に生成者マークと称する）を生成したり、元データと生成者マークとから、前述の第三のマルチメディアデータ（以下、単に生成者署名データと称する）を生成したりする。さらに、通信網100を介して、情報認証者120や情報閲覧者130とデータのやり取りを行う。

【0045】なお、本明細書を実現する場合の生成者マークのデータ形式は限定されず、人間が見ることができて、かつ、データを埋め込むことができるものであればよい。具体的には、BMP、JPEGなど既存のデータ形式を使用することが可能である。また、静止画、動画、さらには、複数枚の静止画を順番に切り替え表示するデータ形式であってもよい。

【0046】端末140₂は、情報認証者120が使用する端末である。情報認証者120は、端末140₂を使って、情報生成者110が生成した元データに対する認証者マークを生成したり、元データと認証者マークとから、前述の第三のマルチメディアデータ（以下、単に認証者署名データと称する）を生成したりする。さらに、通信網100を介して、情報生成者110とデータのやり取りも行う。上記元データと認証者マークとから第三のマルチメディアデータを生成する方法については後述する。

【0047】端末140₃は、情報閲覧者130が使用する端末である。端末140₃は、情報閲覧者130に、文書データや画像データなどを表示する表示装置141と、情報閲覧者130がデータや命令などを入力するための入力装置142₁や142₂（以下、単に入力装置142とも称する）を備えている。情報閲覧者130は、端末140₃を使って、生成者署名データ（または、認証者署名データ）を、生成者マーク（または、認証者マーク）と元データとに分離したり、生成者マーク（または、認証者マーク）を検証したり、元データを閲覧したりする。さらに、通信網100を介して、情報生成者110とデータのやり取りを行う。上記生成者署名データ（または、認証者署名データ）を生成者マーク（または、認証者マーク）と元データとに分離する方法については後述する。

【0048】次に、本実施形態の認証システムを構成する端末140を図面を参照して詳細に説明する。

【0049】図2は、端末140のハードウェア構成を示す図である。

【0050】本実施形態の端末140のハードウェア構成は、図2に示すように、表示装置141と、入力装置142と、通信網インタフェース201と、記憶装置202と、中央処理装置（CPU）203と、一時記憶装置（メモリ）204とが、バス200によって互いに接続されて構成されている。

【0051】表示装置141は、端末140を使用する

情報生成者110、情報認証者120、あるいは情報閲覧者130（以下、全てを纏めて単に利用者とも称する）に各種データを表示するために用いられるものであり、CRTや液晶ディスプレイなどで構成される。

【0052】入力装置142は、端末140を使用する利用者がデータや命令などを入力するために用いられるものであり、キーボードやマウスなどで構成される。

【0053】通信網インターフェース201は、通信網100を介して他の端末とデータのやり取りを行うためのインタフェースである。

【0054】記憶装置202は、端末140で使用されるプログラムやデータを永続的に記憶するために用いられるものであり、ハードディスクやフロッピーディスクなどで構成される。

【0055】CPU203は、端末140を構成する各部を統括的に制御したり、様々な演算処理を行ったりする。

【0056】メモリ204には、オペレーティングシステム204a（以下、単にOS204aとも称する）や、アプリケーションプログラム204b、あるいは真正性保証プログラム204cなどといった、CPU203が上記の処理をするために必要なプログラムなどが一時的に格納される。

【0057】OS204aは、端末140全体の制御を行うために、ファイル管理やプロセス管理、あるいはデバイス管理といった機能を実現するためのプログラムである。

【0058】アプリケーションプログラム204bは、元データを生成、閲覧したり、通信網100を介して他の端末とデータのやり取りを行ったりするためのプログラム群である。

【0059】真正性保証プログラム204cは、生成者マーク（または、認証者マーク）を生成するためや、生成者マーク（または、認証者マーク）と元データとから、生成者署名データ（または、認証者署名データ）を生成するためや、生成者マーク（または、認証者マーク）を検証してその結果を表示するためのプログラムである。すなわち、情報生成者110は、該真正性保証プログラム204cを使って、生成者マークと生成者署名データとを生成する。また、情報認証者120は、該真正性保証プログラム204cを使って、認証者マークと認証者署名データとを生成する。さらに、情報閲覧者130は、該真正性保証プログラム204cを使って、生成者署名データ（認証者署名データ）から生成者マーク（認証者マーク）を分離した後、該生成者マーク（認証者マーク）を用いて元データの真正性を検証するとともに、その結果を表示する。

【0060】端末140₁ないし140₃上で動作するアプリケーションプログラム204bと真正性保証プログラム204cは、上記すべての処理を行なえるものでな

くても良く、同じマルチメディアデータを扱えるものであって、自端末に必要な処理を行なえるものであればよい。また、端末140₁ないし140₃は、同一でなくとも良く、それぞれの端末に必要な機能を持っていればよい。

【0061】また、以下の説明で各アプリケーションプログラム、真正性保証プログラム204cの各動作はオペレーティングシステムの制御の元で行われることもある。

【0062】次に、本実施形態の認証システムの動作について説明する。

【0063】図3は、情報生成者110が生成した元データの真正性を、情報閲覧者130が生成者署名データを用いて検証する場合の、情報生成者110と情報閲覧者130の動作を説明するための図である。

【0064】図3において、情報生成者110が行う処理には端末140₁が使用され、情報閲覧者130が行う処理には端末140₃が使用される。

【0065】まず、情報生成者110は、情報閲覧者130に伝達する元データを生成する（ステップ300）。次に、該元データの真正性を保証する生成者マークを生成し（ステップ301）、当該元データと生成者マークとから生成者署名データを生成する（ステップ302）。そして、該生成者署名データを情報閲覧者130に送信する（ステップ303）。上記情報生成者110の処理の詳細については、後ほど、図4を用いて説明する。

【0066】生成者署名データを受け取った情報閲覧者130は（ステップ304）、まず、該生成者署名データを元データと生成者マークとに分離し（ステップ305）、該生成者マークが確かに情報生成者110によって生成されたものであるか否かを検証する（ステップ306）。そして、該検証結果を確認するとともに（ステップ307）、元データを確認し（ステップ308）、全ての処理を終了する。上記情報閲覧者130の処理の詳細については、後ほど、図5を用いて説明する。

【0067】上記手順において、情報閲覧者130による真正性の確認は、たとえば、図1に示すように表示装置141に「本物です」（あるいは「にせものです」、「生成者マークではありません」）といった吹き出しが表示され、情報閲覧者130が該吹き出しを見ることによって行われる。しかし、本発明自体は、上記表示方法に限定されるものでなく別の表示方法を用いてもよい。たとえば、メッセージボックスやダイアログボックスなどで表示してもよい。また、音などを用いて行ってもよいし、音、表示を組み合わせてもよい。

【0068】さらに、上記手順における、情報生成者110が情報閲覧者130に対して生成者署名データを送る際の、送信手段は、本発明では限定しない。オンライン（たとえば、電子メールなど）であつてもオフライン

(たとえば、フロッピーディスクの郵送など)であつてもよい。また、たとえば、情報生成者110がWebサーバを使って公開している生成者署名データを、情報閲覧者130がブラウザプログラムを使って自発的に取りに行くようにしてもよい。

【0069】図4は、図3における情報生成者110側の処理の詳細を示す図である。

【0070】図4において、一重枠と二重枠とは、それぞれデータとプログラム処理とを表している。

【0071】情報生成者110側の処理は、元データ400を生成するアプリケーションプログラム(マルチメディアデータ処理プログラム)204b1と、該元データ400に対応する生成者署名データ407を生成する真正性保証プログラム204cと、該生成者署名データ407を情報閲覧者に渡すアプリケーションプログラム(通信プログラム)204b2とが連携して行ふ。図4に示すように、本実施例では、アプリケーションプログラム204b1と204b2、および真正性保証プログラム204cとを、それぞれ異なる機能を具備するプログラムとして記載している。しかし、本発明自体は、上記形態に限定されるものではない。たとえば、アプリケーションプログラム204b1とアプリケーションプログラム204b2とが一つのプログラムであってもよい。また、真正性保証プログラム204cが、アプリケーションプログラム204b1のアドイン(プラグイン)プログラムまたは、マクロプログラムであってもよい。

【0072】まず、アプリケーションプログラム204b1は、生成した(元データの生成300)元データ400を、真正性保証プログラム204cに渡す。該二つのプログラム間での元データ400の受け渡し方法としては、アプリケーションプログラム204b1が元データ400をファイルとして記憶装置に書き込み、真正性保証プログラム204cが該記憶装置から読み取るといった方法が考えられる。しかし、本発明自体は、上記方法に限定されるものではなく、メモリを介して受け渡してもよい。

【0073】次に、真正性保証プログラム204cは、該元データ400を所定の圧縮関数を使って圧縮して圧縮子401を生成した後、該圧縮子401に対して情報生成者110の秘密鍵402を使ってデジタル署名処理403を施し、元データ400に対する情報生成者110のデジタル署名404を生成する。上記手順のように、元データ400に直接デジタル署名を施すのではなく、その圧縮子401に対してデジタル署名を施すという手法は、デジタル署名処理にかかる時間を減らすために一般的に行われているものである。しかし、本発明自体は、上記処理方法に限定されるものでなく、元データ400に対して直接デジタル署名を施すようにしてもよい。

【0074】なお、上記圧縮関数には、たとえば、ハッシュ関数のような不可逆性のもでも良いし、可逆性のもでも良い。

【0075】次に、真正性保証プログラム204cは、上記情報生成者110のデジタル署名404と画像データ405とから、生成者マーク406を生成する(生成者マークの生成301)。上記画像データ405は、情報閲覧者130の表示装置141において検証結果表示時に表示されるものであり、たとえば、ロゴマークや印影のようなものである。なお、上記画像データ405の生成は、画像データを処理可能なアプリケーションプログラムを用いて別途行つておく。上記デジタル署名404と画像データ405とを一纏めにする手法としては、たとえば、「IBM SYSTEMS JOURNAL, VOL35, NOS3&4, 1996」の313ページから336ページに記載されているような電子透かし技術の利用が可能である。電子透かしは、画像データに微少な変更を加えることで、情報を埋め込む技術である。本発明において、デジタル署名404と画像データ405とを一纏めにする手段として電子透かしを用いる場合、画像データの視認性(人がその画像データを見て感じ取る情報)さえ阻害しなければ、画像データ自体は多少変形されてもよい。しかし、本発明自体は、上記手法に限定されるものでなく別の手法、例えばハイパーリンクのような関連づけの方法を用いてもよい。

【0076】次に、真正性保証プログラム204cは、上記生成者マーク406と元データ400とから生成者署名データ407を生成する(生成者署名データの生成302)。生成者署名データ407を生成する手法としては、たとえば、図7に示すように、ヘッダ情報を付して二つのマルチメディアデータを単純に結合して、生成者署名データ用フォーマットに変換し、さらにデータ名の一部である拡張子を変換する方法がある。ヘッダ情報とは、真正性保証プログラム204cによって生成される属性情報であり、上記二つのデータをあとで正しく分離するために必要な、該二つのデータの大きさや元々のファイル名などを含んでいる。図7において真正性保証プログラム204cが生成者署名データ407を生成する際の処理の流れを図11に示す。

【0077】図11において、真正性保証プログラム204cは、まず、元データに関する情報と生成者マークに関する情報とを調べ(ステップ1100、1101)、該情報に基づいてヘッダ情報を生成する(ステップ1102)。そして、該ヘッダ情報と元データ、および生成者マークを結合して生成者署名データを生成する(ステップ1103)。上記手順において、三つのデータの結合は、たとえば、ヘッダ情報の最後尾に元データの先頭を連結し、さらに、該元データの最後尾に生成者マークの先頭を連結するような方法で行う。

【0078】また、生成者マーク406と元データ40

0とを一纏めにする際に、上記図7に示すように生成者署名データ用フォーマットに変換して一つのデータにするのではなく、図8に示すように、タグなどリンク情報を用いて元データと生成者マークとを単に関連付けるだけでもよい。ただし、本発明自体は、上記二つの手法に限定されるものでなく別の方法を用いてもよい。

【0079】再び、図4を参照して情報生成者110側の処理の詳細を説明する。

【0080】真正性保証プログラム204cは、上記生成者署名データ407を生成したら、次に、該生成者署名データ407をアプリケーションプログラム204b2に渡す。該二つのプログラム間での生成者署名データ407の受け渡し方法としては、真正性保証プログラム204cが生成者署名データ407をファイルとして記憶装置に書き込み、アプリケーションプログラム204b2が該記憶装置から読み取るといった方法が考えられる。しかし、本発明自体は、上記方法に限定されるものではなく、メモリを介して受け渡してもよい。もちろん、真正性保証プログラム204cは、該生成者署名データ407をアプリケーションプログラム204b1に戻しても良い。

【0081】最後に、アプリケーションプログラム204b2は、生成者署名データ407を情報閲覧者130に送信する（生成者署名データの送信303）。

【0082】図5は、図3における情報閲覧者130側の処理の詳細を示す図である。

【0083】図5において、一重枠と二重枠とは、それぞれデータとプログラム処理とを表している。

【0084】情報閲覧者130側の処理は、生成者署名データ407を受け取るアプリケーションプログラム（通信プログラム）204b2と、該生成者署名データ407を用いて元データ400の真正性を検証する真正性保証プログラム204cと、元データ400を表示するアプリケーションプログラム（マルチメディアデータ処理プログラム）204b1とが連携して行う。図5に示すように、本実施例では、アプリケーションプログラム204b1と204b2、および真正性保証プログラム204cとを、それぞれ異なる機能を具備するプログラムとして別々に記載している。しかし、本発明自体は、上記形態に限定されるものではない。たとえば、アプリケーションプログラム204b1とアプリケーションプログラム204b2とが一つのプログラムであってもよい。また、真正性保証プログラム204cが、アプリケーションプログラム204b1のアドイン（プラグイン）プログラムやマクロプログラムであってもよい。

【0085】まず、アプリケーションプログラム204b2は、生成者署名データ407を受け取り（生成者署名データの受信304）、該生成者署名データ407を真正性保証プログラム204cに渡す。該二つのプログラム間での生成者署名データ407の受け渡し方法とし

ては、アプリケーションプログラム204b2が生成者署名データ407をファイルとして記憶装置に書き込み、真正性保証プログラム204cが該記憶装置から読み取るといった方法が考えられる。しかし、本発明自体は、上記方法に限定されるものではなく、メモリを介して受け渡してもよい。

【0086】ところで、上記処理手順において、生成者署名データ407が前記図7に示すような方法によって一つのデータに纏められている場合、アプリケーションプログラム204b2（情報閲覧者130）は、受け取ったデータ名の拡張子を調べることによって、当該データが生成者署名データ407であると判断することができる。一方、生成者署名データ407が前記図8に示すようにタグなどによって関連付けられている場合には、アプリケーションプログラム204b2（情報閲覧者130）は、情報生成者110から受け取ったデータが生成者署名データ407であるかどうかをすぐには判断できない。しかし、後者の場合においても、アプリケーションプログラム204b2が、受け取った画像ファイルを真正性保証プログラム204cを用いて必ず検証するようにすれば、その結果を見ることによって、該データが生成者署名データ407であるかどうかを判断することができる。生成者署名データ407ではなく単なるマークならば誰も保証していないものであるということを明示するようにしてもよい。

【0087】また、前記図8のHTMLファイル内の画像データに付されるタグを、当該画像データが生成者署名データ407であることを示すための専用タグとしてもよい。ただし、そのような場合には、あらかじめアプリケーションプログラム204b2を、該専用タグが付けられた画像データを受け取った場合に、当該画像データを真正性保証プログラム204cに渡して処理させるように設定しておくことが必要となる。

【0088】次に、真正性保証プログラム204cは、上記生成者署名データ407を元データ400と生成者マーク406とに分離し、（生成者署名データの分離305）、該元データ400を上記所定の圧縮関数を使って圧縮して圧縮子500を生成する。

【0089】上記分離方法は、前述の図4における「生成者署名データの生成302」に対応した方法を用いる。たとえば、前記図7に示す方法によって生成者署名データ407を生成した場合は、真正性保証プログラム204cは、図12に示す処理を行う。

【0090】図12において、真正性保証プログラム204cは、まず、生成者署名データ407の中のヘッダ情報を読み取る（ステップ1200）。そして、該ヘッダ情報の内容にしたがって、生成者署名データ407をヘッダ情報と元データ、および生成者マークに分離する（ステップ1201）。上記手順において、ヘッダ情報から必要な情報が読み取れないなど、何らかのエラーが

発生した場合には、その旨を情報閲覧者130に通知して処理を終了する。

【0091】一方、前記図8に示すように二つのデータをタグなどによって単に関連付けて、生成者署名データ407を生成した場合には、生成者署名データ407を元データ400と生成者マーク406とに分離する処理は行わない。

【0092】再び、図5を参照して情報閲覧者130側の処理の詳細を説明する。

【0093】真正性保証プログラム204cは、次に、該生成者マーク406から情報生成者110のデジタル署名404を抽出し（生成者デジタル署名の抽出501）、さらに、上記圧縮子500と情報生成者110の公開鍵502を使って、該デジタル署名404が確かに情報生成者110が生成したものであるか否かを検証する（デジタル署名の検証503）。上記処理を適正に行うために、情報閲覧者130は、情報生成者110の公開鍵502をあらかじめ入手しておくか、この時点で入手するものとする。入手方法としては、あらかじめ情報生成者110に会って、直接入手する方法が考えられる。しかし、本発明自体は、上記入手方法に限定されるものでなく、たとえば、「SECURE ELECTRONIC COMMERCE（著者：Warwick Ford, Michael S. Baum, 発行書：Prentice Hall PTR）」の193ページから261ページに記載されているような認証機関（Certification Authority）と電子証明書（Public Key Certificate）を利用してもよい。すなわち、電子証明書は公開鍵をも含むので、この電子証明書の入手によって公開鍵を入手することができる。

【0094】電子証明書を入手する方法としては、情報閲覧者130が認証機関から情報生成者110の電子証明書を直接入手する方法や、前記図4で生成者マーク406を生成する際にデジタル署名404と画像データ405に加えて情報生成者110の電子証明書も併せて一纏めにしておき、真正性保証プログラム204cが生成者マーク406から情報生成者110のデジタル署名404を抽出する際に併せて情報生成者110の電子証明書を抽出する方法などがある。

【0095】次に、真正性保証プログラム204cは、上記検証結果を表示装置141に表示する（検証結果の表示307）。該表示は、情報生成者110が指定した画像データ405と検証の結果とから成り、たとえば、図1のようなものである。すなわち、上記検証において、デジタル署名140が正しく検証できれば、元データ400が真正なものであると表示する。また、正しく検証できなければ、元データ400は真正なものではないと表示する。さらに、生成者マーク406の中にデジタル署名404が含まれておらず、検証処理が実行

できなかった場合には、その旨を表示する。情報閲覧者130は、これら表示を見ることによって元データ400が真正なものであるか否かを判断することができる。

【0096】次に、真正性保証プログラム204cは、上記元データ400をアプリケーションプログラム204b1に渡す。該二つのプログラム間での元データ400の受け渡し方法としては、真正性保証プログラム204cが元データ400をファイルとして記憶装置に書き込み、アプリケーションプログラム204b1が該記憶装置から読み取るといった方法が考えられる。しかし、本発明自体は、上記方法に限定されるものではなく、メモリを介して受け渡してもよい。

【0097】最後に、アプリケーションプログラム204b1は、元データ400を表示装置141に表示する（元データの表示308）。該表示に関しては、真正性保証プログラム204cが、元データ400のファイル名（拡張子）などから起動すべきアプリケーションプログラムを確認し、アプリケーションプログラム204b1に元データ400を渡すとともに該アプリケーションプログラム204b1を起動することによって、自動的に表示するようにすると便利である。

【0098】上記手順は、ステップ307と、ステップ308の処理順序を限定するものではない。

【0099】また、上記手順において、図9に示すように、元データ400と画像データ（検証結果を含む）との表示処理を、アプリケーションプログラムと真正性保証プログラムとが、それぞれ別々に行っている。しかし、本発明は、上記方法に限定されるものではない。アプリケーションプログラムが画像データも表示可能である場合には、図10に示すように、元データと画像データとを該アプリケーションプログラムによって表示してもよい。その場合には、真正性保証プログラム204cは、元データだけでなく画像データをもアプリケーションプログラムに渡す。ただし、アプリケーションプログラムが、画像データを表示する場合でも、前記真正性保証プログラムは、画像データと検証結果との表示を行う。

【0100】上記の本実施形態では、情報生成者110は、任意のアプリケーションプログラムを使って生成した元データ400に対し、該元データ400の真正性を保証するデジタル署名404を生成した後、画像データ405とまとめて生成者マーク406を生成するようにしている。そして、該生成者マーク406と元データ400とをまとめて情報閲覧者130に渡すようにしている。

【0101】また、情報閲覧者130は、受け取った生成者マーク406に含まれる情報生成者110のデジタル署名404を用いて、併せて受け取った元データ400の真正性を検証するようにしている。さらに、該検証結果が視覚、聴覚などによって情報閲覧者130に伝

えられるようにしている。

【0102】したがって、本発明によれば、不正者が元データ400を改ざんしたり、生成者マーク406を別の情報に付けかえたりした場合には、デジタル署名404の検証処理でエラーとなり、それが視覚、聴覚などで情報閲覧者130に伝えられる。結果として、情報閲覧者130は、元データ400が真正なものであるか否かを正しく確認することができる。

【0103】次に、本発明の他の実施形態が適用された認証システムの動作について説明する。

【0104】図6は、情報生成者110が生成した元データに対して、情報認証者120が該元データの真正性を保証する認証者署名データを生成し、さらに情報閲覧者130が該認証者署名データを用いて元データの真正性を検証する場合の、情報生成者110と情報認証者120、および情報閲覧者130の動作を説明するための図である。

【0105】図6において、情報生成者110が行う処理には端末140₁が使用され、情報認証者120が行う処理には端末140₂が使用される。また、情報閲覧者130が行う処理には端末140₃が使用される。

【0106】まず、情報生成者110は、アプリケーションプログラムを使って情報閲覧者130に伝達する元データを生成する(ステップ600)。そして、該元データを情報認証者120に送信する(ステップ601)。

【0107】元データを受け取った情報認証者120は(ステップ602)、該元データの真正性を保証する認証者マークを生成し(ステップ603)、当該元データと認証者マークとから認証者署名データを生成する(ステップ604)。そして、該認証者署名データを情報生成者110に返送する(ステップ605)。

【0108】情報生成者110は、情報認証者120から返送されてきた認証者署名データを(ステップ606)情報閲覧者130に送信する(ステップ607)。

【0109】認証者署名データを受け取った情報閲覧者130は(ステップ608)、該認証者署名データを元データと認証者マークとに分離し(ステップ609)、該認証者マークが確かに情報認証者110によって生成されたものであるか否かを検証する(ステップ610)。そして、該検証結果を確認するとともに(ステップ611)、元データを適切なアプリケーションプログラムによって確認し(ステップ612)、全ての処理を終了する。

【0110】上記手順において、認証者マークの生成処理(ステップ603)、および認証者署名データの生成処理(ステップ604)は、図4に示す生成者マークの生成処理(ステップ301)、および生成者署名データの生成処理(ステップ302)と基本的に同じである。また、認証者署名データの分離処理(ステップ609)、認証者マ

ークの検証処理(ステップ610)、および検証結果・元データの確認処理(ステップ611、612)については、図5に示す生成者署名データの分離処理(ステップ305)、生成者マークの検証処理(ステップ306)、および検証結果・元データの確認処理(ステップ307、308)と基本的に同じである。その他、図6における、ステップ600、607、608は、それぞれ、図3のステップ300、303、304に相当する。

【0111】また、上記手順では、情報生成者110から情報認証者120に対して元データを送っているが、情報生成者110側で元データの圧縮子を生成し、該圧縮子を情報認証者に送るようにしてもよい。この場合は、元データの内容が、情報認証者にはわからないようにすることができる。

【0112】上記の本実施形態では、情報認証者120は、情報生成者110が任意のアプリケーションプログラムを使って生成した元データの真正性を保証するデジタル署名を生成した後、画像データと一纏めにして認証者マークを生成するようにしている。そして、該認証者マークと元データとを一纏めにして情報生成者110に渡すようにしている。

【0113】また、情報生成者110は、情報認証者120から返送された認証者マークと元データを情報閲覧者130に渡すようにしている。

【0114】さらに、情報閲覧者130は、受け取った認証者マークに含まれる情報認証者120のデジタル署名を用いて、併せて受け取った元データの真正性を検証するようにしている。加えて、該検証結果が視覚、聴覚などによって情報閲覧者130に伝えられるようにしている。

【0115】したがって、本発明によれば、不正者が元データを改ざんしたり、認証者マークを別の情報に付けかえたりした場合には、デジタル署名の検証処理でエラーとなり、それが視覚、聴覚などで情報閲覧者130に伝えられる。結果として、情報閲覧者130は、元データが真正なものであるか否かを正しく確認することができる。

【0116】なお、本発明は、上記各実施例に限定されるものではなく、その要旨の範囲内で様々な変形が可能である。

【0117】たとえば、本発明では、検証結果の如何に依らず元データを表示するようにしているが、本発明はこれに限定されない。検証の結果、元データの真正性が確認された場合に、適切なアプリケーションプログラムを使って元データを表示するようにしてもよい。この場合は、図5において、ステップ307の結果によって、ステップ308の処理が制御されることになる。

【0118】また、本発明では、真正性保証プログラムが生成者署名データを受け取った場合に自動的に検証処理を行うようにしているが、本発明はこれに限定されな

い。情報閲覧者が明示的に指示を出したときに行うようにしてもよい。そのような場合、真正性保証プログラムは、生成者マークの代わりに、検証処理が済んでいない生成者マークがあることを示すための独自の画像データを表示するようにすると、情報閲覧者にわかりやすく便利である。

【0119】さらに、上記各実施例では、画像データとデジタル署名とを一纏めにする場合について説明しているが、文字データ、画像データ、ビデオデータ、音データなどのマルチメディア、さらにはこれらを組み合わせたマルチメディアデータにも適用可能であることは自明である。

【0120】加えて、上記各実施例では、元データ（または、元データの圧縮子）をデジタル署名の対象としているが、本発明はこれに限定されない。たとえば、該元データの有効期限や、原本、謄本の区別などといった属性情報を生成し、該属性情報と元データとをデジタル署名の対象としてもよい。

【0121】例えば、元データがある期間内だけ有効であり、それを過ぎると効力を失うようなものであった場合、元データと生成者マーク（認証者マーク）、ならびに有効期限から生成者署名データ（認証者署名データ）を生成し、検証結果を情報閲覧者に伝える際に有効期限も併せて伝えるようにしてもよい。

【0122】また、原本の保管場所（物理的な場所（例えば住所）と論理的な場所（例えばURL）のどちらでもよい）を生成者署名データ（認証者署名データ）の生成要素の一つとし、検証の際に、上記保管場所の情報を用いて、当該閲覧データが原本であるか謄本であるかを判断し、署名検証結果を情報閲覧者に伝える際に、その判断結果を併せて伝えるようにしてもよい。

【0123】また、元データに対するアクセス制御情報を属性情報に含めることもできる。アクセス制御情報を含めた場合、真正性保証プログラムは、当該アクセス制御情報を参照して情報閲覧者が当該元データを見る権利があるかどうかを判断し、権利がある場合にアプリケーションプログラムに元データを渡すようにする。この場合、さらに、元データを情報生成者側で暗号化し、情報閲覧者に見る権利がある場合に復号するようにしてもよい。

【0124】さらに、本発明では、情報閲覧者の端末で真正性の検証処理を行っているが、本発明はこれに限定されない。たとえば、情報生成者がインターネットのようなオープンなネットワーク上で公開している情報（生成者署名データ）を、あるポリシーによって管理されているドメイン内（例えば、企業や学校など）の情報閲覧者が見る場合に、当該ドメインのドメイン内ネットワークとインターネットとの間に設置されているファイアウォール等のゲートウェイ装置で真正性の検証処理を行ってもよい。その場合、さらに、真正性が確認されない情

報はドメイン内ネットワークに流さないようにしたり、特定のマークが付加されている情報以外はドメイン内ネットワークに流さないようにしたりすると、安全性や利便性が高まる。

【0125】また、上記各実施例の各端末に格納された各プログラムは、一般的には、それぞれの装置を制御するオペレーティングシステムの下で動作し、オペレーティングシステムを介して、装置の各ハードウェア構成要素とデータ、コマンドをやり取りする。もちろん、オペレーティングシステムを介さずに直接、各ハードウェア構成要素とデータ、コマンドのやり取りをしてもよい。

【0126】加えて、これらのプログラムが各端末に格納される際に、フロッピーディスク、CD-ROM、DVD等各種記憶媒体に格納された形態で供給されるか、あるいはこれらの端末が接続されたネットワークに接続された他の端末からダウンロードされることがある。

【0127】さらに加えて、本発明では、通信網100を流れるデータを暗号化してはいないが、情報の機密性を保証するために別途暗号通信を行ってもよい。

【0128】以上説明したように、本発明によれば、第一のユーザが生成したマルチメディアデータの真正性を、第二のユーザが視覚、聴覚などによって正しく確認することができる。

【0129】

【発明の効果】以上説明したように、本発明によれば、第一のユーザが生成したマルチメディアデータが真正なものであるか否かを、そのマルチメディアデータのフォーマットやそれを処理するアプリケーションプログラムに依らず、第二のユーザが視覚、聴覚などで直接的に確認することができるので、安全性を確保することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態が適用された認証システムの概略構成を示す図である。

【図2】図1に示す端末のハードウェア構成を示す図である。

【図3】本発明の第1の実施形態が適用された認証システムにおいて、情報生成者が生成した元データの真正性を情報閲覧者が検証する際の動作を説明するためのフロー図である。

【図4】図3に示す情報生成者の処理の詳細を示す図である。

【図5】図3に示す情報閲覧者の処理の詳細を示す図である。

【図6】本発明の他の実施形態が適用された認証システムにおいて、情報生成者が生成した元データの真正性を情報認証者が保証するとともに、該真正性を情報閲覧者が検証する際の動作を説明するためのフロー図である。

【図7】生成者マークと元データとを一纏めにする方法の一例を示す図である。

【図 8】生成者マークと元データとを一纏めにする方法の別の例を示す図である。

【図 9】元データと画像データ、および検証結果を表示する方法の一例を示す図である。

【図 10】元データと画像データ、および検証結果を表示する方法の別の例を示す図である。

【図 11】元データと生成者マークとを生成者署名データに纏める際の真正性保証プログラムの処理の流れの一例を示すフロー図である。

【図 12】生成者署名データを元データと生成者マークとに分離する際の真正性保証プログラムの処理の流れの一例を示すフロー図である。

【符号の説明】

100：通信網

110：情報生成者

120：情報認証者

130：情報閲覧者

140 (140₁~140₃)：端末

141：表示装置

142：入力装置

200：バス

201：通信網インターフェース

202：記憶装置

203：CPU

204：メモリ

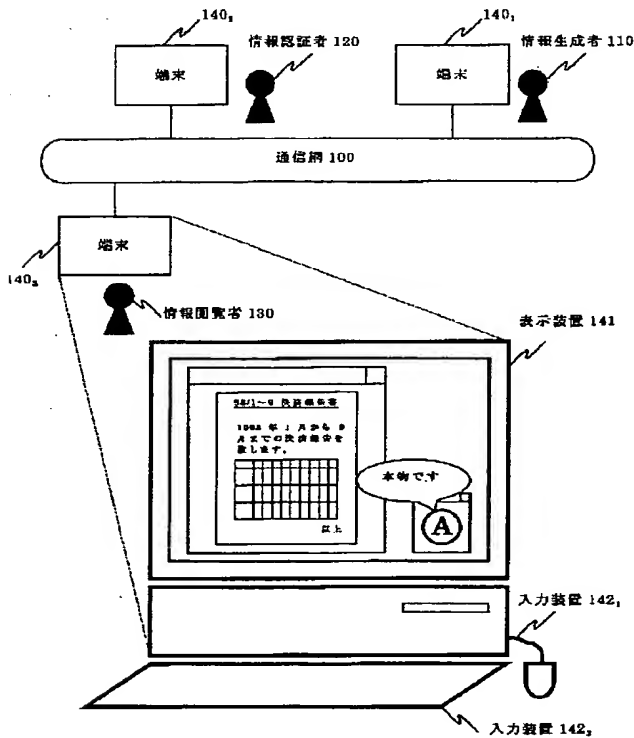
204a：オペレーティングシステム

204b：アプリケーションプログラム

204c：真正性保証プログラム

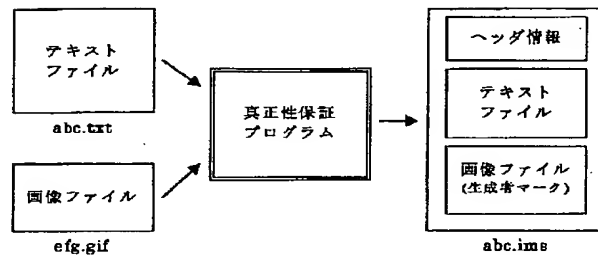
【図 1】

図 1



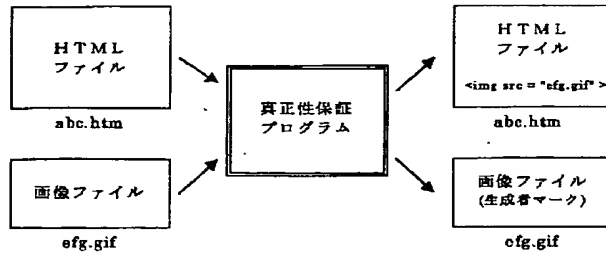
【図 7】

図 7



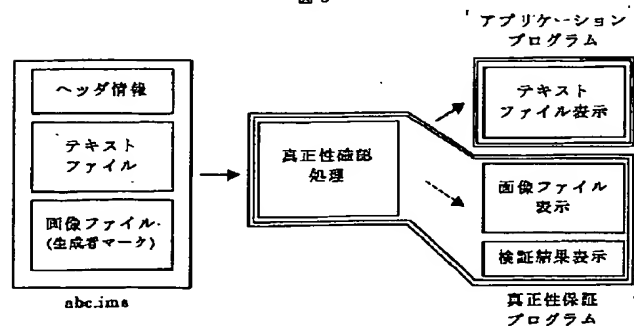
【図 8】

図 8



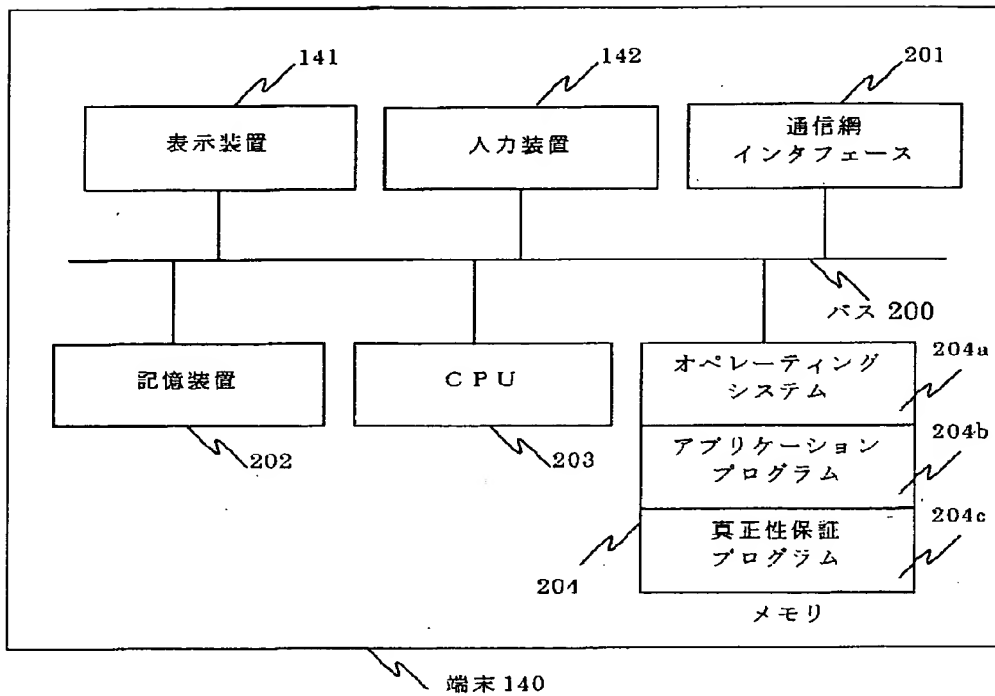
【図 9】

図 9



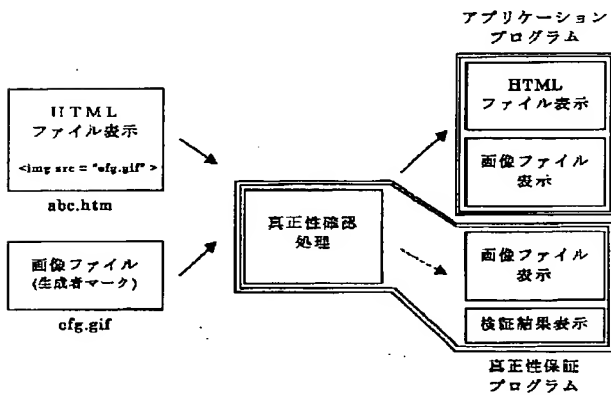
【図2】

図 2



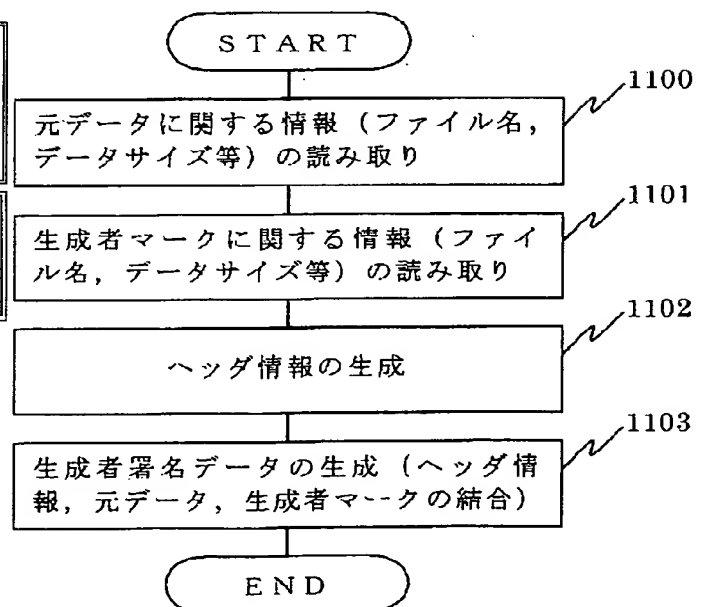
【図10】

図10



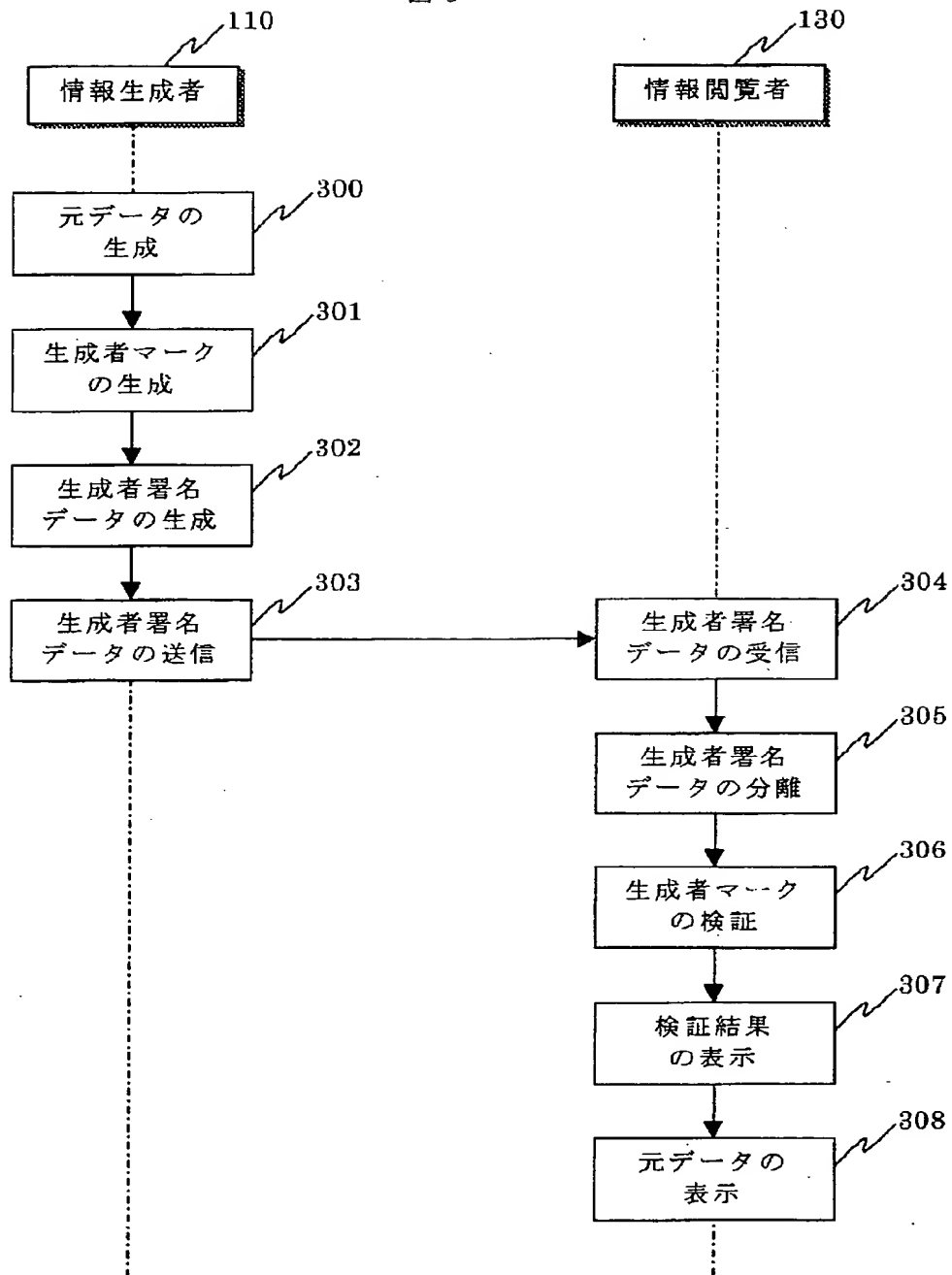
【図11】

図11



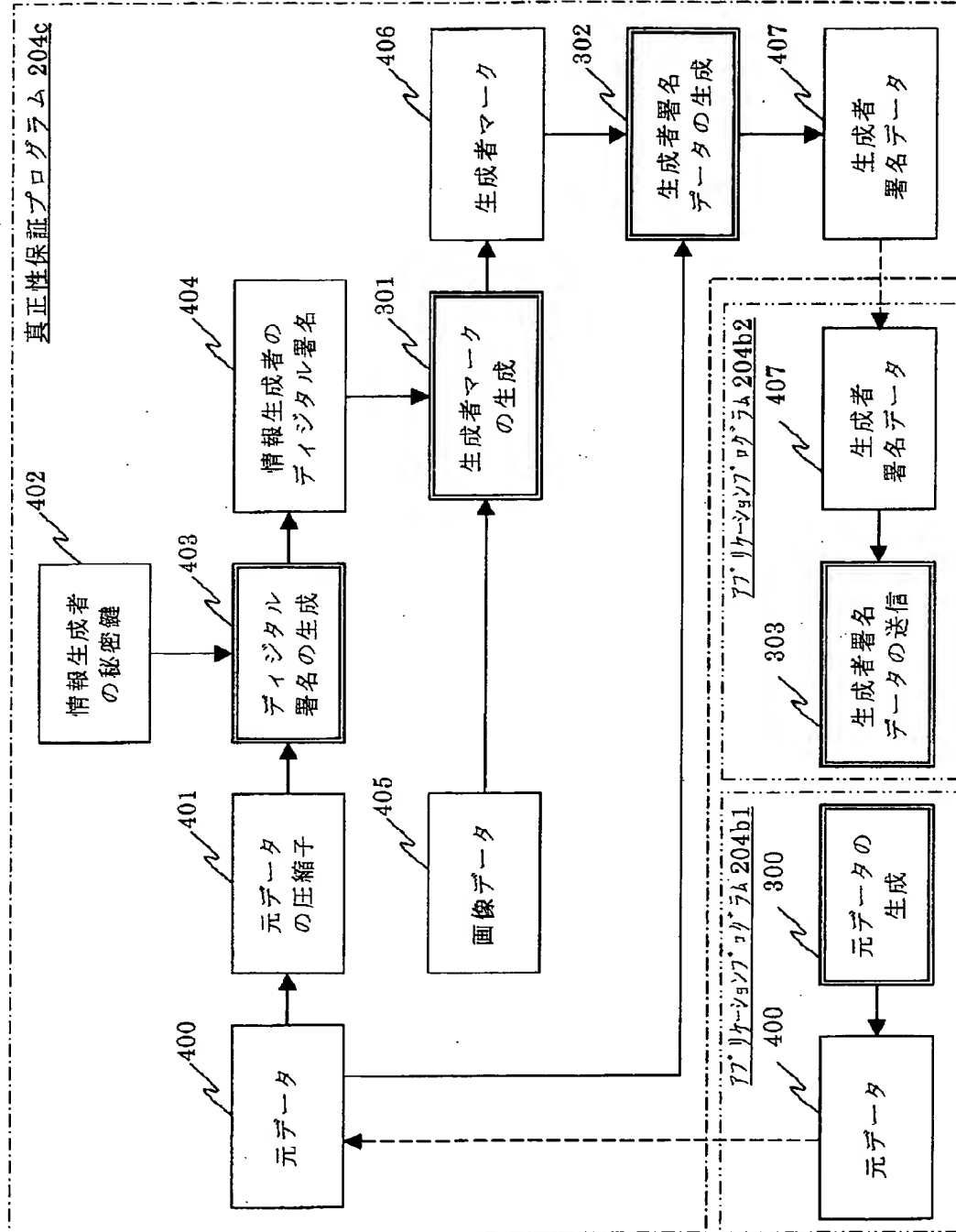
【図 3】

図 3



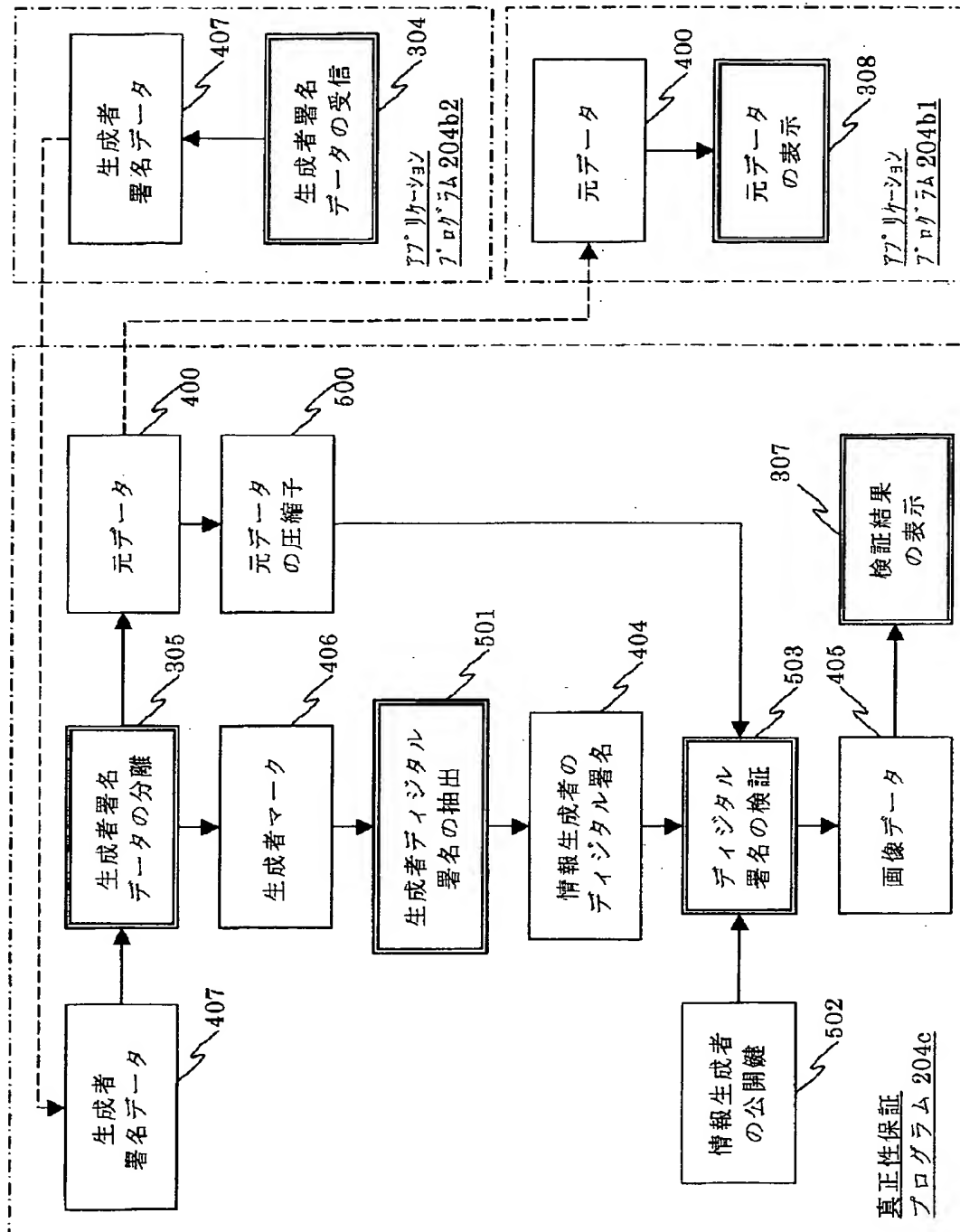
【図 4】

図 4

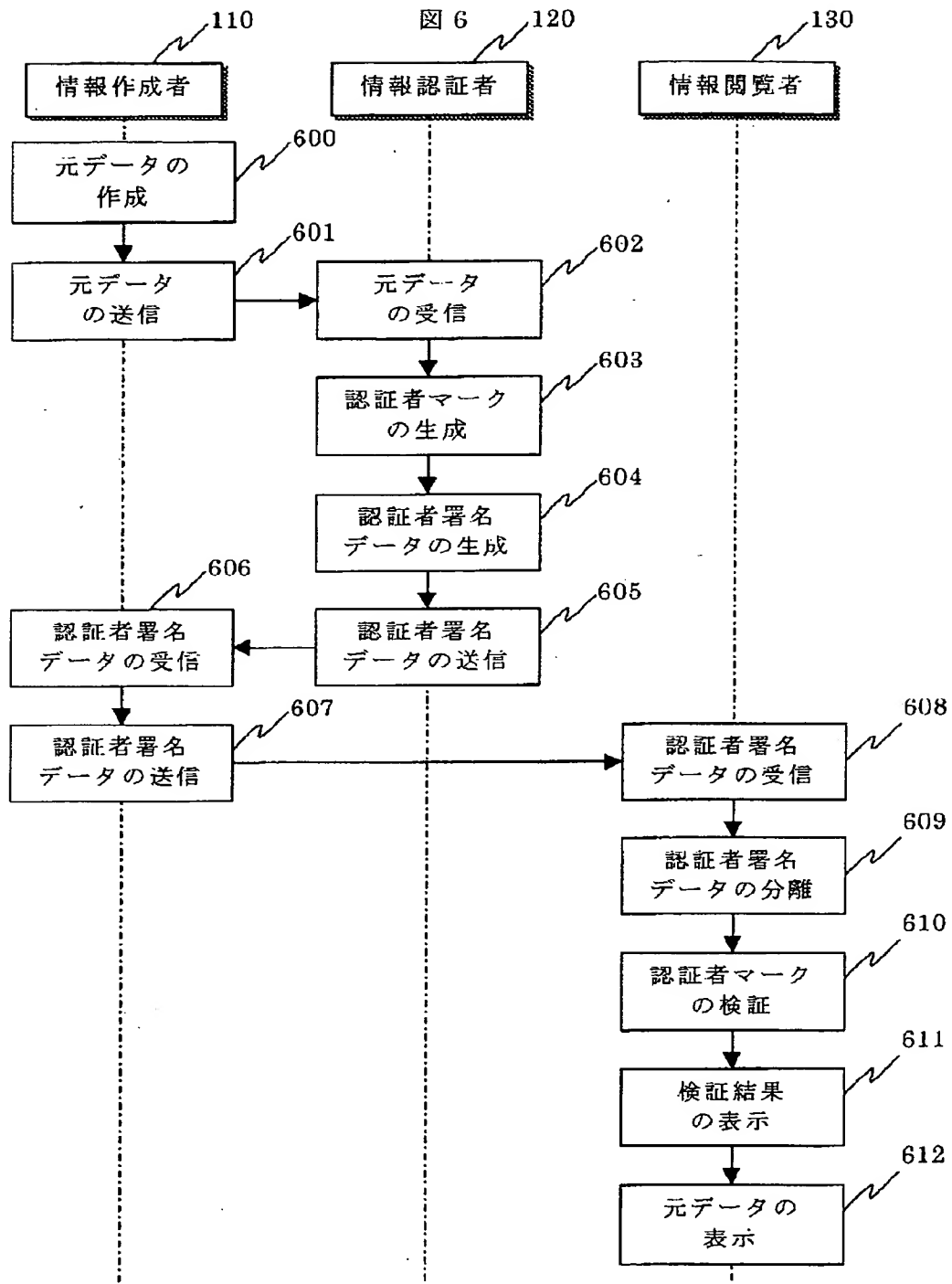


【図5】

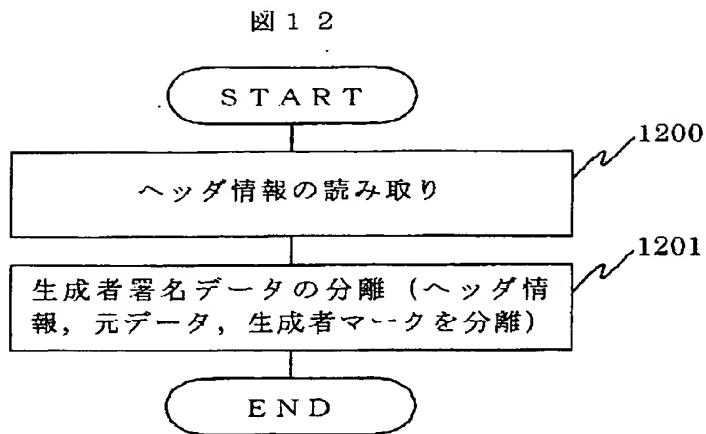
図5



【図6】



【図 12】



フロントページの続き

(51) Int. Cl. 7

識別記号

F I

テーマコード (参考)

H 0 4 L 9/32

H 0 4 L 9/00

6 7 5 B

(72) 発明者 長野 裕美

東京都江東区新砂一丁目 6 番 27 号 株式会
社日立製作所公共情報事業部内

(72) 発明者 豊田 英樹

神奈川県横浜市戸塚区戸塚町 5030 番地 株
式会社日立製作所ソフトウェア事業部内

(72) 発明者 鍛 忠司

神奈川県川崎市麻生区王禅寺 1099 番地 株
式会社日立製作所システム開発研究所内